

DEP Documentation

RSA Key Generation User Manual

[illegible]

CONFIDENTIALITY

The information in this document is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Atos Worldline S.A./N.V.

COPYRIGHT

The information in this document is subject to change without notice and shall not be construed as a commitment by Atos Worldline S.A./N.V.

The content of this document, including but not limited to trademarks, designs, logos, text, images, is the property of Atos Worldline S.A./N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the other applicable Acts.

The contents of this document must not be reproduced in any form whatsoever, by or on behalf of third parties, without the prior written consent of Atos Worldline S.A./N.V.

Except with respect to the limited license to download and print certain material from this document for non-commercial and personal use only, nothing contained in this document shall grant any license or right to use any of Atos Worldline S.A./N.V.'s proprietary material.

LEGAL DISCLAIMER

While Atos Worldline S.A./N.V. has made every attempt to ensure that the information contained in this document is correct, Atos Worldline S.A./N.V. does not provide any legal or commercial warranty on the document that is described in this specification. The technology is thus provided "as is" without warranties of any kind, expressed or implied, included those of merchantability and fitness for a particular purpose. Atos Worldline S.A./N.V. does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed.

To the fullest extent permitted under applicable law, neither Atos Worldline S.A./N.V. nor its affiliates, directors, employees and agents shall be liable to any party for any damages that might result from the use of the technology as described in this document (including without limitation direct, indirect, incidental, special, consequential and punitive damages, lost profits).

JURISDICTION AND APPLICABLE LAW

These terms shall be governed by and construed in accordance with the laws of Belgium. You irrevocably consent to the jurisdiction of the courts located in Brussels for any action arising from or related to the use of this document.

TABLE OF CONTENTS

1. SCOPE OF THE DOCUMENT	5
1.1. REFERENCES	5
1.2. CONTACTING ATOS WORLDLINE	5
2. PURPOSE OF RSA KEY GENERATION PROGRAM	6
3. USE OF RSA KEY GENERATION	6
3.1. PREREQUISITES	6
3.2. START-UP	6
3.3. DESCRIPTION.....	7
3.4. COMMUNICATION	7
3.5. HOW TO GENERATE AN RSA KEY	8
3.6. ERRORS DURING EXECUTION.....	11
3.6.1. <i>Validation of input data</i>	11
3.6.2. <i>Validation of the DEP Crypto Module</i>	12
3.6.3. <i>Error code from the DEP Crypto Module</i>	12
4. ANNEX A: INSTALLATION PROCEDURE	14
5. ANNEX B: NOTATIONS	17

1. SCOPE OF THE DOCUMENT

This document describes how to generate RSA keys (RSA Key Pair and RSA Public Key) using the *RSA Key Generation* program.

The document doesn't explain the functionalities of the DEP libraries on which this program is based.

1.1. REFERENCES

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to:

- *DEP Host Interface Protocol*
- *DEP/NMS User Manual*
- *DEP/Linux User Manual*
- *DEP/T6 Owner Manual*

There are no references made to the following documents, but they could be useful to understand this document:

- *PKI Library for DEP - Reference DFS Manual*
- *DEP Introduction to DEP*
- *DEP General Architecture*
- *DEP Glossary*

1.2. CONTACTING ATOS WORLDLINE

You can visit *Atos Worldline* on the World Wide Web to find out about new products and about various other fields of interest.

URL: www.atosworldline.com.

For the documentation visit <http://www.banksys.com> web page.

For support on issues related to DEP, customers, partners, resellers, and distributors can send an email to the DEP Hotline:

<mailto:deph hotline-atosworldline@atosorigin.com>.

2. PURPOSE OF RSA KEY GENERATION PROGRAM

The purpose of this program is to generate RSA Keys (RSA Key Pair and RSA Public Key) and write it in specific files.

The program is intended to be used on a PC (running on Microsoft Windows 2000, Windows 2000 and Windows Vista) that is connected to a DEP Platform (DEP/T6) loaded with a DEP Application Software that can generate and export RSA Keys. It also can be added as a plug-in in DEP/NMS application.

3. USE OF RSA KEY GENERATION

The installation procedure is reported to the *AnnexA on page 14*.

3.1. PREREQUISITES

- The DEP Crypto Module must be unlocked;
- A valid DEP Application Software should be loaded on DEP Crypto Module;
- A DEP Application Software that supports the generation and export of RSA Keys should be loaded on DEP Crypto Module;
- The **K_PKI_RSA_TRANSPORT_KEY** or the **K_PKI_RSA_TK_AES** transport key should be loaded in DEP Crypto Module depending on the export method to be chosen (DES or AES);
- To use the RSA Key Generation application as a DEP/NMS plug-in, the USB License Dongle must be present.

3.2. START-UP

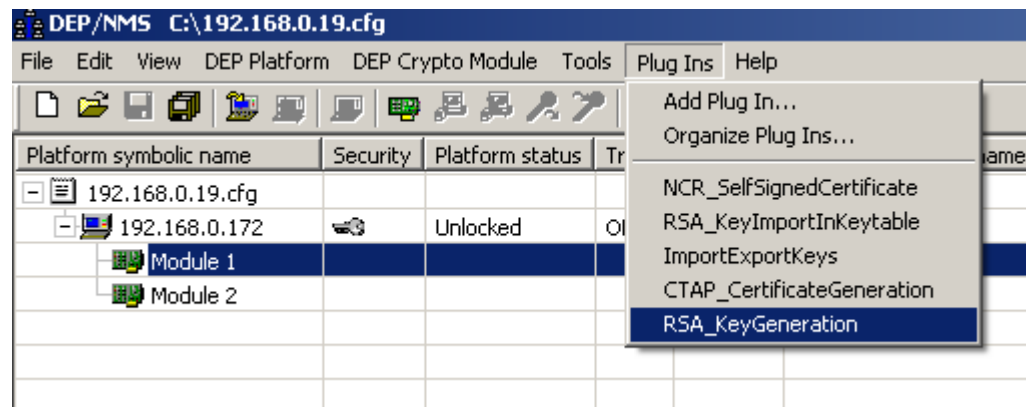
The *RSA Key Generation* can be launched by executing:

**C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\RSA Key
Generation\RSA_KeyGeneration.exe**

This is the default path. It is possible to define another path during installation (paragraph 4 on page 14).

The application can also be launched directly through the *DEP/NMS*. Select the appropriate DEP Crypto Module and run the *RSA_KeyGeneration* plug-in from the

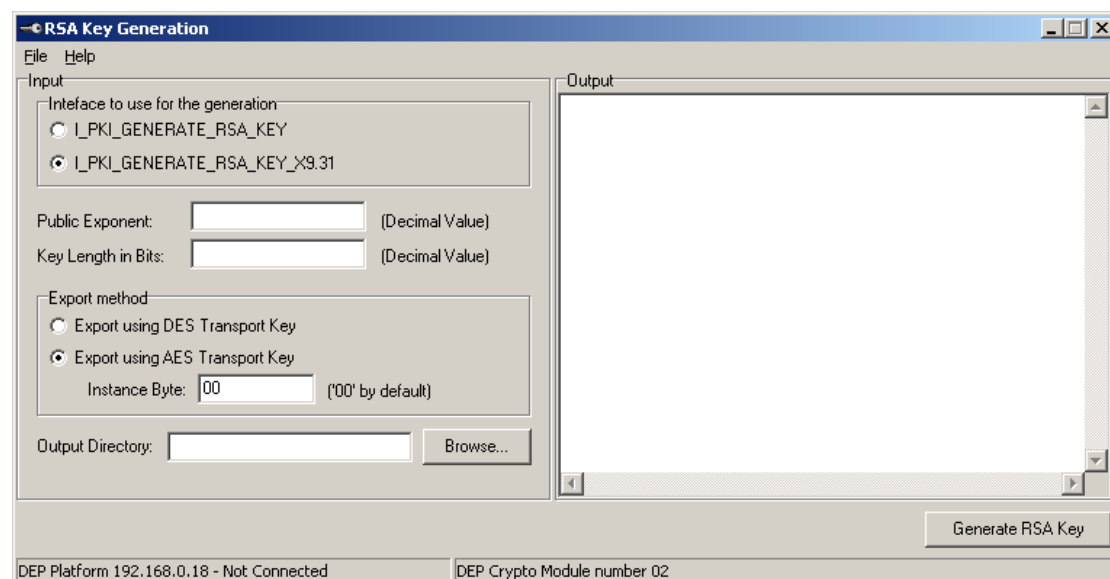
Plug Ins menu.



Before starting the application, the communication must be defined. (See paragraph 3.3 on page 7).

3.3. DESCRIPTION

Once the RSA Key Generation program is started, the following window is opened:



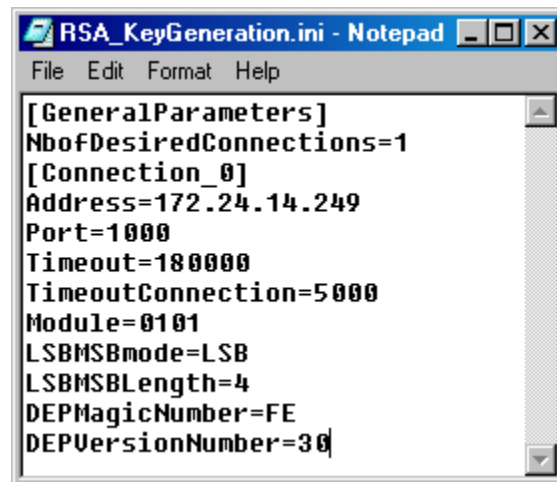
A menu at the top of the window allows to have a look at the program version (and also contact the DEP Hotline), the help files or to exit.

The *Input* section contains the list of parameters needed to generate an RSA Key (see paragraph 3.4 on page 8). The *Output* section (blank part) will log the operations and their results.

3.4. COMMUNICATION

If the application is launched by the DEP/NMS, the communication is automatically set by the *DEP/NMS* program.

If the application is used as stand-alone application, the user should set the general parameters and the connection settings in the *RSA_KeyGeneration.ini* configuration file.



- *NbOfDesiredConnections* must be set to '1'.
- *Address* represents the IP address of the target DEP platform.
- *Port* represents the TCP/IP port used for the communication with the DEP platform.
- *TimeOut* represents the maximum waiting time in milliseconds for the response from the DEP Crypto Module.
- *TimeOutConnection* represents the maximum waiting time in milliseconds for establishing a connection.
- *Module* represents the DEP Crypto Module used to generate the RSA Key: the first byte will be always '01' and the second byte defines the target module: '01' to '04'.
- The four last parameters are described in the DEP Documentation (*DEP Host Interface Protocol*)

3.5. HOW TO GENERATE AN RSA KEY

All the fields of the left panel must be filled.

Field Name	Length	Description	Format
Public Exponent	5	Public exponent for the RSA Key to generate. The maximum value is 4294967295 (=FFFFFFFF _{hex}).	n10
Key Length in Bits	2	Length of the RSA Key to generate (value max 4096 depending on the hardware of the DEP Crypto Module).	n4
Instance Byte	1	Instance of AES transport key to be used in export	h2
Output Directory	/	Existing directory in which the RSA key files will be stored.	/

User must select interface to be used for RSA Key generation. If I_PKI_GENERATE_RSA_KEY interface is selected, the standard way of RSA key generation will be used. If I_PKI_GENERATE_RSA_KEY_X9.31 interface is selected, the ANSI X.9.31 specification-based RSA key generation way will be used.

Note: The private part of the RSA key generated is encrypted before export.

User must select the exporting method to be used for export of the RSA Key generated. If 'Export using DES Transport key' is selected, then the private part of the RSA key generated will be encrypted by using DES transport key. If 'Export using AES Transport key' is selected, then the private part of generated RSA key will be encrypted by using the appropriate instance of AES transport key.

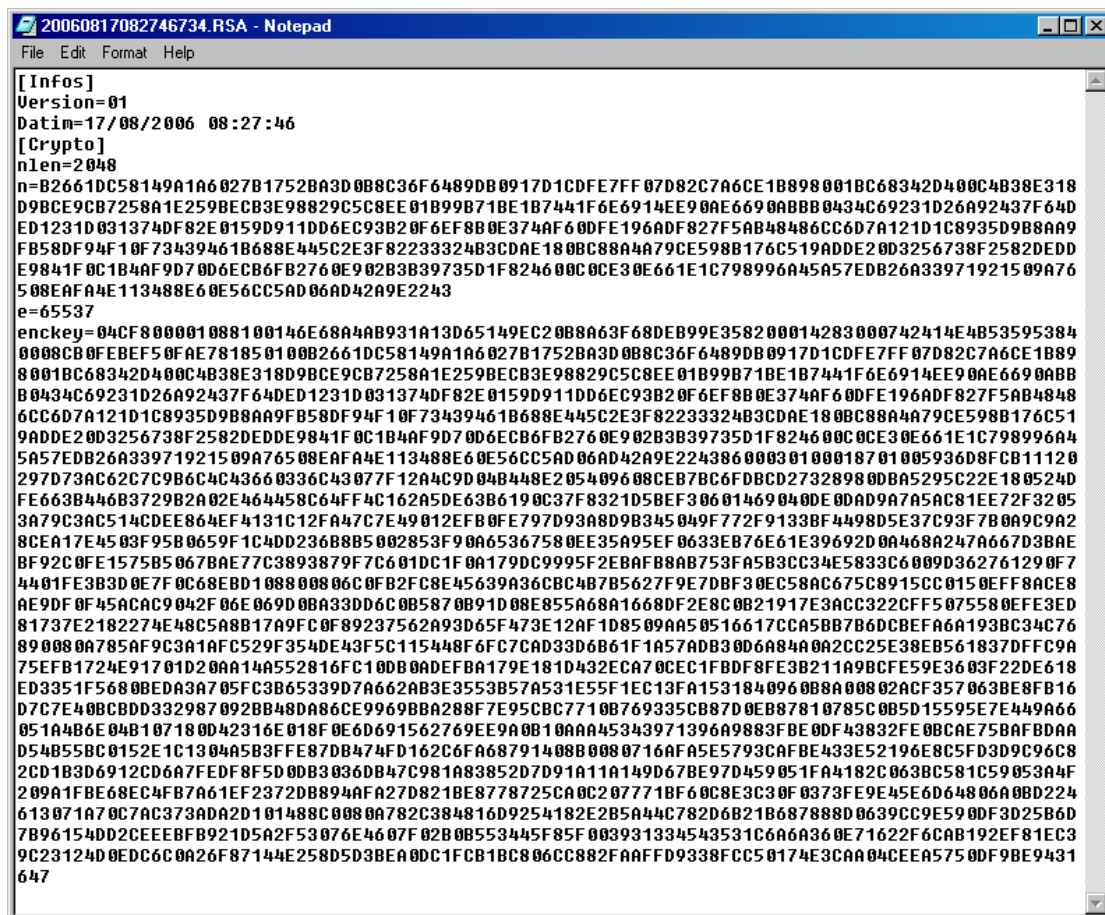
When the user clicks the **Generate RSA Key** the TCP/IP connection to the DEP Crypto Module is established and the key is generated.

The right panel shows the progress of the generation:

- The validation of the input data,
- The status of the call sent to the DEP Crypto Module,
- The modulus of the RSA key generated,
- The name of the files generated by the application (.RSA, .PUB),
- The name of the log file,
- The eventual errors.

Below are shown the structures of three generated files.

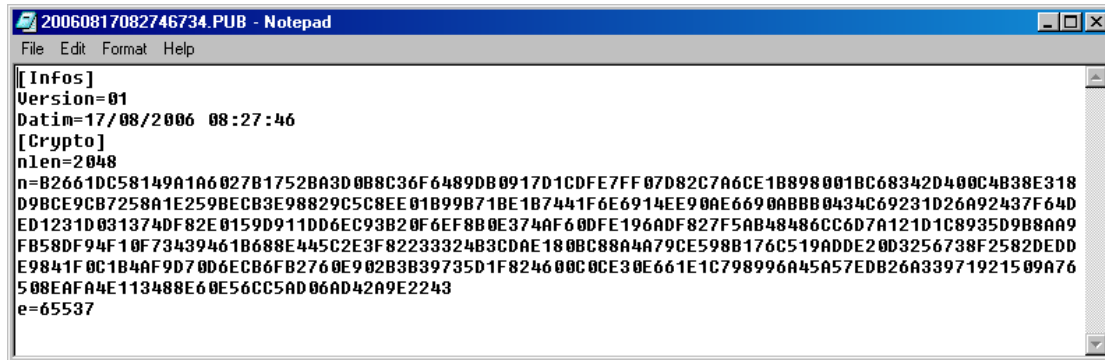
1. The “.RSA” file contains the entire RSA Key Pair. (The Private part of the key is encrypted).



```
20060817082746734.RSA - Notepad
File Edit Format Help

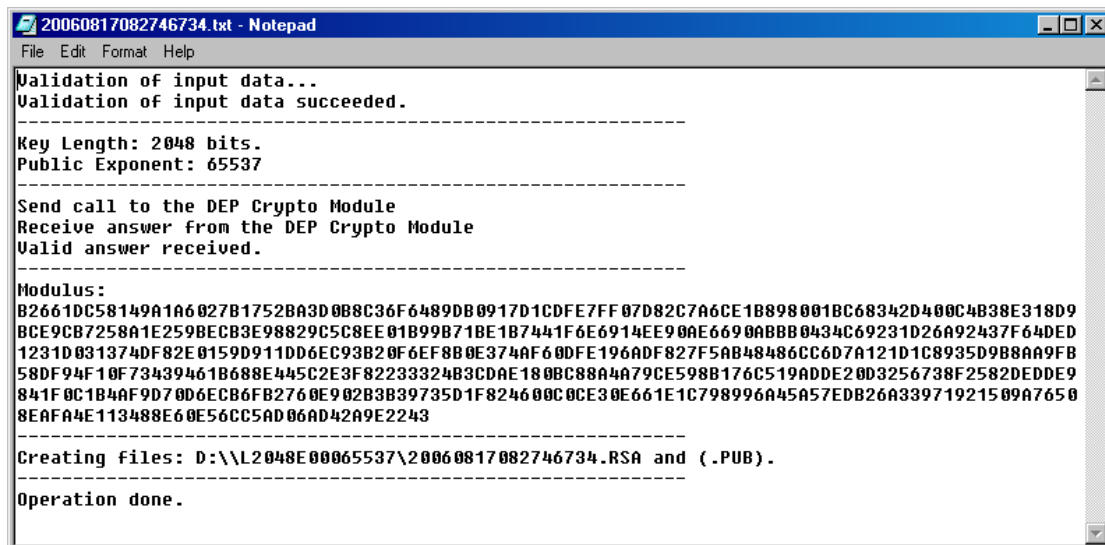
[Infos]
Version=01
Date=17/08/2006 08:27:46
[Crypto]
nlen=2048
n=B2661DC58149A1A6027B1752BA3D0B8C36F6489DB0917D1CDFE7FF07D82C7A6CE1B898001BC68342D400C4B38E318
D9BCE9CB7258A1E259BECB3E98829C5C8EE01B99B71BE1B7441F6E6914EE90AE6690ABBB0434C69231D26A92437F64D
ED1231D031374DF82E0159D911DD6EC93B20F6EF8B0E374AF60DFE196ADF827F5AB48486CC6D7A121D1C8935D9B8AA9
FB58DF94F10F73439461B688E445C2E3F82233324B3CDAE180BC88A4A79CE598B176C519ADDE20D3256738F2582EDD
E9841F0C1B4AF9D70D6ECB6F82760E902B3B39735D1F824600C0CE30E661E1C798996A45A57EDB26A33971921509A76
508EAF4A4E113488E60E56CC5AD06AD42A9E2243
e=65537
encKey=04CF800001088100146E68A4AB931A13D65149EC20B8A63F68DEB99E358200014283000742414E4B53595384
0008CB0FEBEF50FAE781850100B2661DC58149A1A6027B1752BA3D0B8C36F6489DB0917D1CDFE7FF07D82C7A6CE1B89
8001BC68342D400C4B38E318D9BCE9CB7258A1E259BECB3E98829C5C8EE01B99B71BE1B7441F6E6914EE90AE6690ABBB
0434C69231D26A92437F64DED1231D031374DF82E0159D911DD6EC93B20F6EF8B0E374AF60DFE196ADF827F5AB4848
6CC6D7A121D1C8935D9B8AA9FB58DF94F10F73439461B688E445C2E3F82233324B3CDAE180BC88A4A79CE598B176C51
9ADDE20D3256738F2582EDDE9841F0C1B4AF9D70D6ECB6F82760E902B3B39735D1F824600C0CE30E661E1C798996A4
5A57EDB26A33971921509A76508EAF4A4E113488E60E56CC5AD06AD42A9E22438600030100018701005936D8FCB1120
297D73AC62C7C9B6C4C43660336C43077F12A4C9D04B448E205409608CEB7BC6FDBCD273289800BA5295C22E180524D
FE663B446B3729B2A02E464458C64FF4C162A5DE63B6190C37F8321D5BEF30601469040DE0DAD9A7A5AC81EE72F3205
3A79C3AC514CDEE864EF4131C12FA47C7E49012EFB0FE797D93A8D9B345049F772F9133BF4498D5E37C93F7B0A9C9A2
8CEA17E4503F9580659F1C4D0236B8B5002853F90A65367580EE35A95EF0633EB76E61E39692D0A468A247A667D3BAE
BF92C0FE1575B5067BAE77C3893879F7C601DC1F0A179DC9995F2EBAF8B8A753FA5B3CC34E5833C6009D362761290F7
4401FE3B3D0E7F0C68EBD108800806C0FB2FC8E45639A36C8C4B7B5627F9E7DBF30EC58AC675C8915CC0150EFF8ACE8
AE9DF0F45ACAC9042F06E069D0BA33D06C0B5870B91D08E855A68A1668DF2E8C0B21917E3ACC322CFF5075580EFE3ED
81737E2182274E48C5A8B17A9FC0F89237562A93D65F473E12AF1D8509AA50516617CCA5BB7B6DCBEFA6A193BC34C76
890080A785AF9C3A1AFC529F354DE43F5C115448F6FC7CAD33D6B61F1A57ADB30D6A84A0A2CC25E38EB561837DFFC9A
75EFB1724E91701D20AA14A552816FC10DB0ADEFB8179E181D432ECA70CEC1FBDFF8FE3B211A9BCFE59E3603F22DE618
ED3351F5680BEDA3A705FC3B65339D7A662AB3E353B57A531E55F1EC13FA15318409600B8A00802ACF357063B8E8FB16
D7C7E40BCBDD332987092BB48DA86CE9969BBA288F7E95CBC7710B769335CB87D0EB87810785C0B5D15595E7E449A66
051A4B6E04B107180D42316E018F0E6D691562769EE9A0B10AAA45343971396A9883FBE0DF43832FE0BCAE75BAFBDAA
D54B55BC0152E1C1304A5B3FFE87DB474FD162C6FA68791408B0080716AFA5E5793CAFBE433E52196E8C5FD3D9C96C8
2CD1B3D6912CD6A7FEDF85D00B3036DB47C981A83852D7D91A11A149D67BE97D459051FA4182C063BC581C59053A4F
209A1FBE68EC4FB7A61EF2372D8894FA27D821BE8778725CA0C207771BF60C8E3C30F0373FE9E45E6D64806A0BD224
613071A70C7AC373ADA2D101488C0080A782C384816D9254182E2B5A44C782D6B21B687888D0639CC9E590DF3D25B6D
7B96154DD2CEEBFB921D5A2F53076E4607F02B0B553445F85F003931334543531C6A6A360E71622F6CAB192EF81EC3
9C23124D0EDC6C0A26F87144E258D5D3BEA0DC1FCB1BC806CC882FAAFFD9338FCC50174E3CAA04CEE5750DF9BE9431
647
```

2. The “.PUB” file contains only the Public Part of the RSA Key.



```
[Infos]
Version=01
Datin=17/08/2006 08:27:46
[Crypto]
nlen=2048
n=B2661DC58149A1A6027B1752BA3D0B8C36F6489DB0917D1CDFE7FF07D82C7A6CE1B898001BC68342D400C4B38E318
D9BCE9CB7258A1E259BECB3E98829C5C8EE01B99B71BE1B7441F6E6914EE90AE6690ABBB0434C69231D26A92437F64D
ED1231D031374DF82E0159D911DD6EC93B20F6EF8B0E374AF60DFE196ADF827F5AB48486CC6D7A121D1C8935D9B8AA9
FB58DF94F10F73439461B688E445C2E3F82233324B3CDAE180BC88A4A79CE598B176C519ADDE20D3256738F2582DEDD
E9841F0C1B4AF9D70D6ECB6FB2760E902B3B39735D1F824600C0CE30E661E1C798996A45A57EDB26A33971921509A76
508EAF4E113488E60E56CC5AD06AD42A9E2243
e=65537
```

- The “.LOG” file contains the text present in the output memo.



```
Validation of input data...
Validation of input data succeeded.

-----

Key Length: 2048 bits.
Public Exponent: 65537

-----

Send call to the DEP Crypto Module
Receive answer from the DEP Crypto Module
Valid answer received.

-----

Modulus:
B2661DC58149A1A6027B1752BA3D0B8C36F6489DB0917D1CDFE7FF07D82C7A6CE1B898001BC68342D400C4B38E318D9
BCE9CB7258A1E259BECB3E98829C5C8EE01B99B71BE1B7441F6E6914EE90AE6690ABBB0434C69231D26A92437F64DED
1231D031374DF82E0159D911DD6EC93B20F6EF8B0E374AF60DFE196ADF827F5AB48486CC6D7A121D1C8935D9B8AA9FB
58DF94F10F73439461B688E445C2E3F82233324B3CDAE180BC88A4A79CE598B176C519ADDE20D3256738F2582DEDD E9
841F0C1B4AF9D70D6ECB6FB2760E902B3B39735D1F824600C0CE30E661E1C798996A45A57EDB26A33971921509A7650
8EAF4E113488E60E56CC5AD06AD42A9E2243

-----

Creating files: D:\L2048E00065537\20060817082746734.RSA and (.PUB).

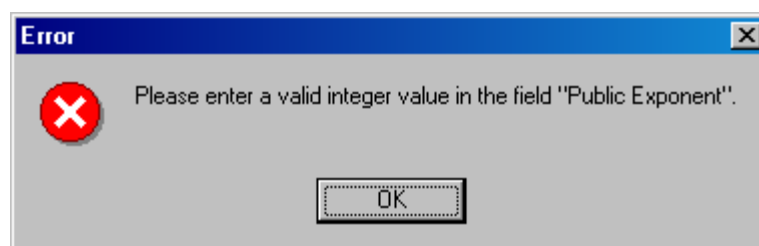
Operation done.
```

3.6. ERRORS DURING EXECUTION

3.6.1. Validation of input data

Before sending the call to the DEP Crypto Module some verifications are made and friendly messages are displayed.

For example:



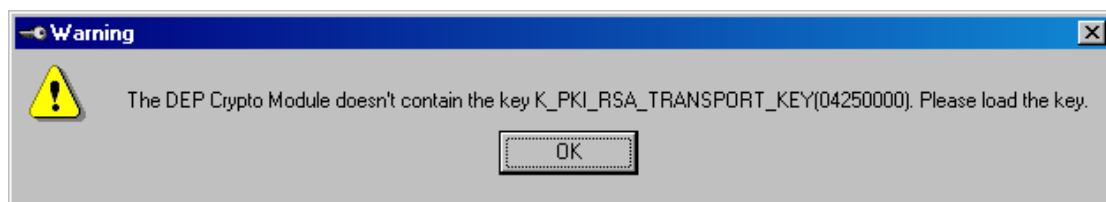
Selecting the **OK** button sets the focus to the erroneous field for correction.

3.6.2. Validation of the DEP Crypto Module

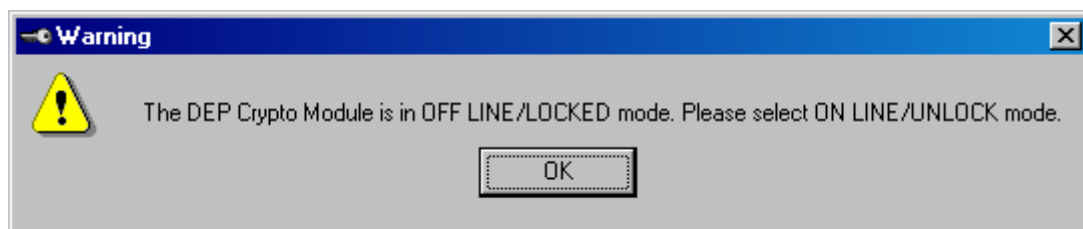
After the input validation, the application performs a DEP Crypto Module validation. The following conditions will be checked:

- If the DEP Crypto Module is on-line/unlocked;
- If the DEP Crypto Module contains a valid DEP Application Software;
- If the DEP Application Software is able to generate and export RSA Keys;
- If the **K_PKI_RSA_TRANSPORT_KEY** (DES transport key) or the **K_PKI_RSA_TK_AES** (AES transport key) key is loaded in the DEP Crypto Module.

If one of the verifications failed, a warning window is displayed:



All warning windows disappear automatically when the problem is solved. For example: when the correct key is loaded or when the DEP Crypto Module is set on-line/unlocked.

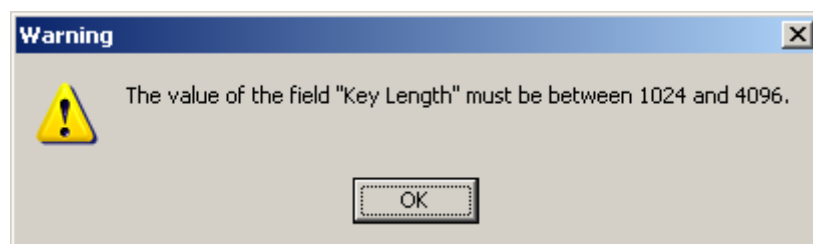


The user can also click on the **OK** button, solve the problem and click again on **Generate RSA Key** button.

3.6.3. Error code from the DEP Crypto Module

After all verifications are done successfully, a call is sent to the DEP Crypto Module. When no problem occurs the RSA Key is generated, otherwise an error message is returned.

For example:



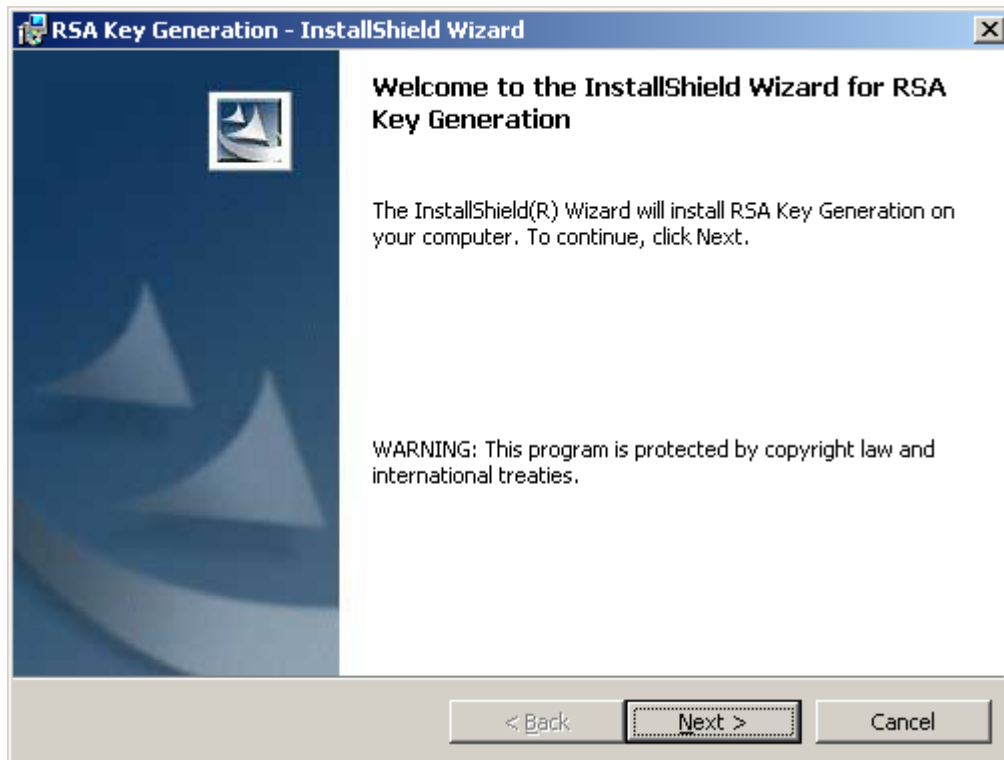
If ANSI X.9.31 specification based RSA key generation is executed on DEP Crypto Module which is not supporting it, the following error message is returned:



4. ANNEX A: INSTALLATION PROCEDURE

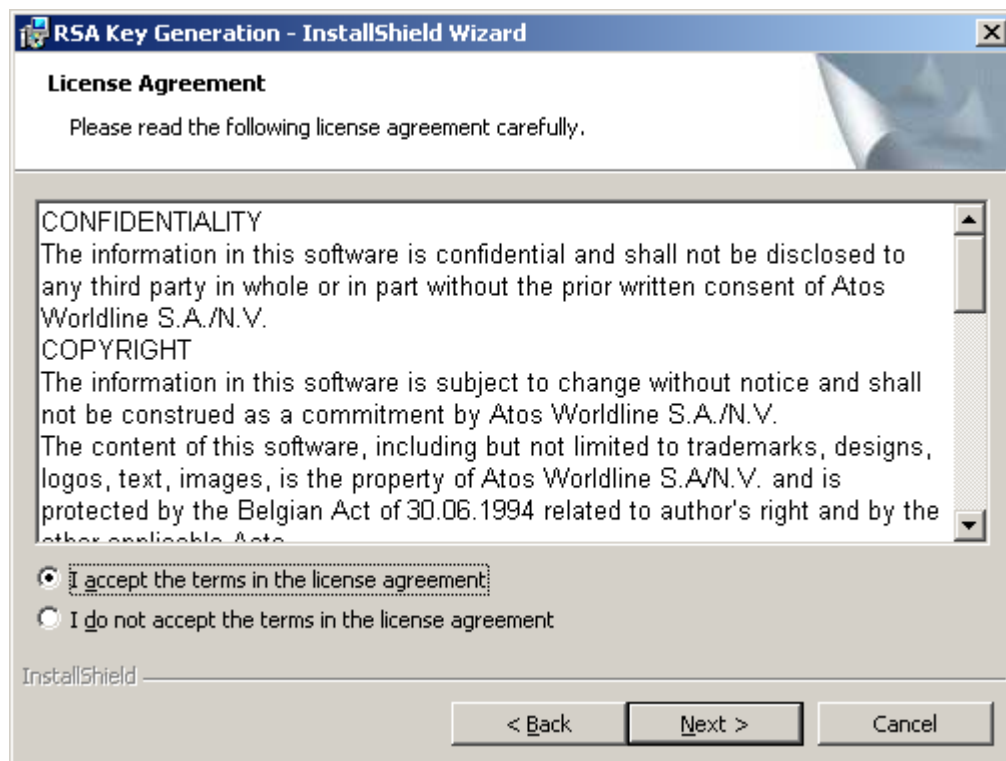
An installation procedure exists for the RSA Key Generation program. It is a wizard-driven procedure that lets you to install the RSA Key Generation program.

To begin the installation wizard, execute the **setup.exe**.



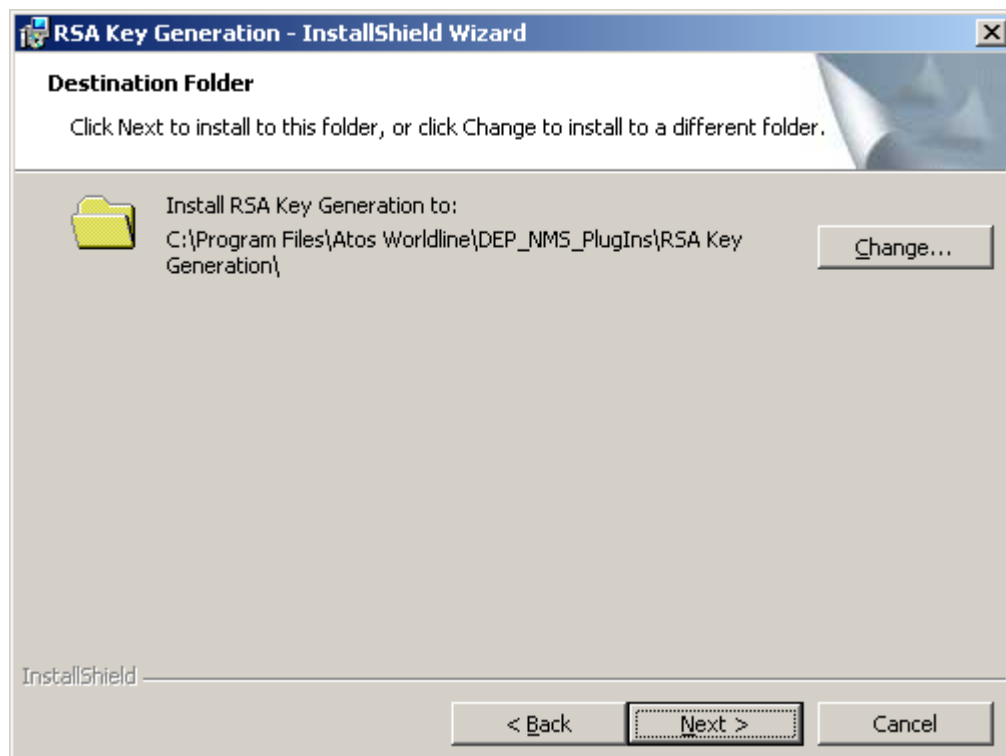
Click **Next** to continue.

Read and accept the License Agreement.



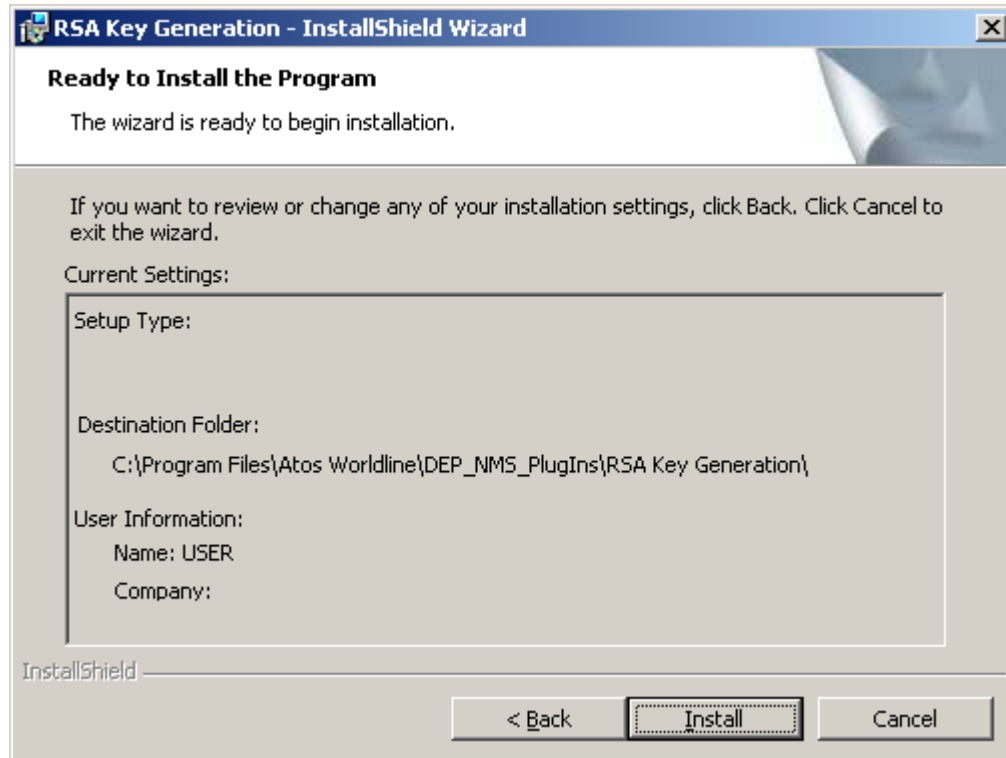
Click **Next** to continue.

The **Destination Folder** window allows defining the path where the application is installed. It is recommended to use the default path, yet you can specify a different folder by clicking **Change...** and selecting the desired folder for the installation.



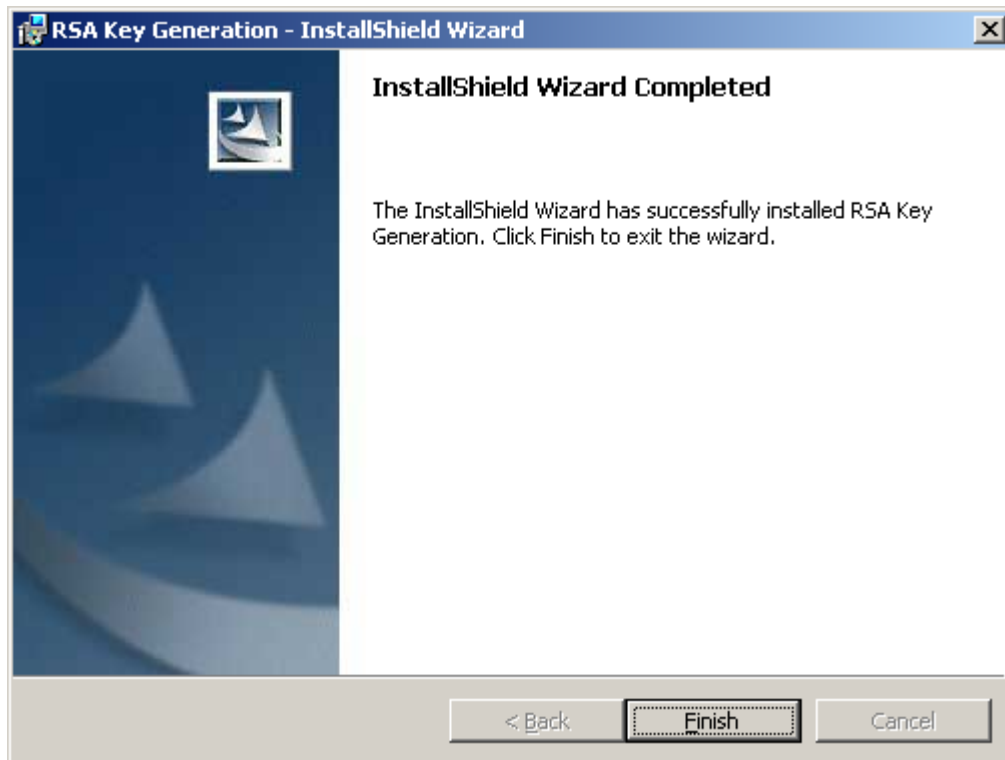
Click the **Next** button.

Click the **Install** button to start an installation process. If you want to return to the previous screen, press **Back** or if you want to abort the procedure, click **Cancel**.



Once you have confirmed the installation options, the actual installation starts.

Click **Finish** to exit the installation procedure.



5. ANNEX B: NOTATIONS

The following abbreviations are used in this document.

n	Numeric
h	Hexadecimal